REMARKS

The present amendment is in response to the Office Action dated January 11, 2008. Claims 4-8, 10, 17, 20-25, 28, 30-33, and 36-39 are now present in this case. By this amendment, claims 4, 5, 7, 10, 21, 25, 28, 30, and 32 have been amended, claims 27 and 35 have been cancelled, and new claim 39 has been added.

Transmitting personalization indicators in an unsecured wireless network can present security issues because such indicators can be intercepted, permitting unauthorized users to access sensitive personal information. (Page 4, lines 19-21.) Further, many users wish to remain anonymous and do not intend to reveal their telephone numbers or other personal data to a content provider. (Page 4, lines 21-23.) Security sensitive user identification parameters include the user's MSISDN (which includes the user's telephone number) and the IMSI (which includes a unique subscriber identifier). (Page 6, lines 12-15.)

While the MSISDN and IMSI are transmitted to the network, it is undesirable to transmit these parameters to a content provider because of security and privacy concerns. (*Id.*; Page 5, lines 21-28.) In other words, the MSISDN and IMSI are not anonymous user identifiers because each contains information about the user. While a mobile terminal's electronic serial number ("ESN") does not reduce network security, it is not necessarily associated with a particular user and as such is not a user identifier. (Page 4, lines 23-27.)

The present application avoids the security and privacy concerns of transmitting the MSISDN or IMSI to a content provider by instead providing a SIM_ID 107 established by the manufacturer that is unrelated to security-sensitive user identification parameters.

Claim Rejections based on 35 U.S.C. § 102

Claims 4-8, 27, 28, 30-33 and 35 stand rejected under 35 U.S.C. § 102(e), first paragraph, as being anticipated by U.S. Patent No. 6,606,491 issued to Peck. Claims 27 and 35 have been cancelled by this amendment.

As an initial comment, Peck is concerned with authentication to a network and not with the identification of a user to a content provider after authentication occurs.

Specifically, Peck teaches an authentication process in which the dual-mode terminal 24 transmits an AUTHR (using an Authentication Word C) that was derived based on the SIM-based ESN and a hidden Shared Secret Data ("SSD"). (Column 7, lines 36-39.) In the background section, the SSD is described as being derived from the A-key and the terminal-based ESN under a procedure described in EIA/TIA 553A. (Column 2, lines 17-19.) Therefore, in the previous amendment filed in this matter, it was assumed the AUTHR value is related to the terminal-based ESN (i.e., a device identifier). However, upon a rereading of the reference, it appears that the "hidden SSD" may be selected in some manner and stored by the network and one of the mobile terminal and the SIM. Because the reference teaches that SSD updates are not required when a user uses a new mobile terminal having a new terminal-based ESN, the reference appears to assume (but does not teach) the SSD is stored on the SIM. (column 8, line 60 to column 9, line 3).

Peck also teaches the subscriber records used by the network to authenticate a subscriber include the SIM-based MIN, A-Key, SSD, terminal-based ESN, and SIM-based ESN. (Column 7, line 61 to column 8, line 8.) However, the reference also teaches the mobile terminal transmits the MIN, AUTHR, and terminal-based ESN. (Column 7, lines 45-46.) Therefore, the only value transmitted present in the subscriber record is the terminal-based ESN. One could infer that Peck teaches the terminal-based ESN is used to locate the correct subscriber record for the purposes of obtaining the A-Key, SSD, and SIM-based ESN to validate the mobile terminal. But, this is at odds with the statement in Peck that the terminal-based ESN "is no longer a part of the validation process." (Column 8, lines 62-64.) If as asserted in the Office Action and claimed by claim 10 of Peck (but not recited anywhere else in the reference), the mobile terminal transmits the SIM-based ESN, this value could be used to locate the correct subscriber record. Further, while not recited in the reference, the mobile terminal may transmit the SIM-based MIN, which could alternatively be used to locate the correct subscriber record.

In short, Peck appears to teach or imply the mobile terminal transmits the MIN, AUTHR, terminal-based ESN, SIM-based ESN, and SIM-based MIN. The terminal-based ESN is a device identifier but not a user identifier. Both the MIN and

SIM-base MIN are telephone numbers of the mobile terminal, which are considered security sensitive information. As explained above with respect to Peck, the SIM-based ESN is used to determine the AUTHR. Therefore, the AUTHR and the SIM-based ESN, which is used to create the AUTHR, are authentication information and are therefore security sensitive information. In other words, by incorporating the SIM-based ESN into the authentication process, Peck has made the SIM-based ESN a piece of security sensitive information related to authentication that could be used by an unauthorized user to gain access to the network.

Amended independent claim 4 recites an anonymous user identifier unrelated to both a device identifier and the authentication information. Because Peck fails to teach or suggest such an anonymous user identifier, Peck fails to anticipate or render obvious the inventions of claim 4 and claims 6, 28, and 30-33 that depend therefrom.

Amended independent claim 7 recites a processor configured to determine an anonymous user identifier unrelated to both the device identifier and the authentication information as a function of the SIM serial number. Because Peck fails to teach or suggest such an anonymous user identifier, Peck fails to anticipate or render obvious the inventions of claim 7 and claims 8 and 36 that depend therefrom.

Claim Rejections based on 35 U.S.C. § 103(a)

Claims 10, 17, 20-25 and 36-38 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,310,889 issued to Parsons et al. in view of Peck.

As acknowledged in the previous Office Action, Parsons et al. fails to teach an anonymous user identifier based on a SIM serial number. Further, Parsons et al. fails to teach an anonymous user identifier. Specifically, Parsons et al. teaches verifying the identify of a user using either an explicit step, such as the user inputting a user ID and password; or an implicit step, such as the connection being to a known address, such as an IP address or Domain Name (DN). (Column 5, lines 19-24.) In a second location, Parsons et al. teaches a personal agent that "provides access to the information necessary to identify the user to network 14, by a user ID and password, a

known IP address, a pager number, a cellular EIN, etc." Therefore, Parsons et al. fails to cure the deficiencies of Peck with respect to claims 10, 17, 20-25 and 36-38.

Independent claim 10 has been amended to recite an anonymous user identifier associated with the SIM serial number and unrelated to both the device identifier and the authentication information. As explained above, Peck does not teach or suggest this claim element. Therefore, Parsons et al., Peck, and the hypothetical combination thereof, fail to render obvious the invention of claim 10. Claims 17, 20, 37, and 38 are also allowable in view of the fact that they depend from claim 10, and further in view of the recitations in each of those claims.

Independent claim 21 has been amended to recite an anonymous user identifier based, at least in part, on a serial number of the SIM and being unrelated to both the device identifier and the authentication information. Therefore, Parsons et al., Peck, and the hypothetical combination thereof, fail to render obvious the invention of claim 21. Claims 22-24 are also allowable in view of the fact that they depend from claim 21, and further in view of the recitations in each of those claims.

Independent claim 25 has been amended to recite selecting an anonymous user identifier based, at least in part, on the serial number of the SIM that is unrelated to both the authentication information and the device identifier. Therefore, Parsons et al., Peck, and the hypothetical combination thereof, fail to render obvious the invention of claim 25.

As explained above, Peck fails to anticipate or render obvious the invention of claim 7. Parsons et al. fails to cure the deficiencies of Peck. Therefore, claim 36 is allowable in view of the fact that it depends from claim 7, and further in view of the recitations of claim 36.

New Claims

New claim 39 is also allowable in view of the fact that it depends from claim 4, and further in view of the recitations in claim 39.

All of the claims remaining in the application are now believed to be allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

The Commissioner is hereby authorized to charge any fees due or credit any overpayment to Deposit Account No. 04-0258 of Davis Wright Tremaine LLP.

If questions remain regarding this application, the Examiner is invited to contact the undersigned at (206) 757-8021.

Respectfully submitted,
Herman Chien
DAVIS WRIGHT TREMAINE LLP

By /Heather M. Colburn/
Heather M. Colburn
Registration No. 50815

1201 Third Avenue
Suite 2200
Seattle, WA 98101-3045
Phone: (206) 757-8021
Facsimile: (206) 757-7021